Amendments to the Specification:

Please correct the typographical error in paragraph [0126] as follows:

[0126] Scam Detector--Much has been written recently about a variety of annoying and even harmful information disseminated throughout the Internet that ranges from simple propagated rumors, misinformation and inaccuracies to deliberate hoaxes or fraudulent scams with malicious intent to profit at the expense of other people who are duped into believing deceptive promises, claims and other information. Some of the most insidious of the latter include the notorious Nigerian bank account scam, aid to US soldiers in Afghanistan, aid to victims' families of the 9/11 tragedy and a variety of charity based scams. Unquestionably, the most abhorring, and in fact, disturbing form of scam involves those dangerous individuals who exploit use of the Internet's very privacy protecting advantages in order to pose as a type of individual (e.g., a teenage girl) which they are in fact not (e.g., while in fact being a 40 year old stalker or even sexual predator of children). In order to address these problems both individually and collectively, what may be needed is a system which may be implemented at the browser or ISP level, which collaboratively and innocuously combs through both specific content and users' behavioral responses and information oriented responses to such information. Accordingly the system is based upon a statistical model containing statistical and NLP components and operates in a fully distributed and collaborative fashion. It observes and compares information using statistical NLP in order to determine the suspicion thresholds of any given content which fits the basic format of a potential scam. The language model may be based upon a set of adaptive rules which are initially manually inputted and which become refined and modified in accordance with relevance feedback. Examples of sources of these rules may include statistical models of "deceptive information" (perhaps from a training corpus). It may also be based upon other pre-existing scams, which have been clearly identified as such. Of course, there are many sub-categories of scams which fit the definition of a scam and each would be modeled individually, for example, false or exaggerated claims made by spam advertisers (i.e., false advertising) traditional Internet scams, Internet rumors or other false information which could become propagated, etc. Although it is not an extremely likely scenario, such a system could also be used in a protective capacity in which, for example, some rogue entity were somehow able to ~~gail~~ gain control over the network (e.g., cyberterrorists) and disseminate apparently legitimate information that could result in a panic or frenzy and/or such entity posing, for example as a government authority figure requesting that individual (or the public) to react in a way that could be particularly harmful to an, entity, government, (e.g., an individual, such as a person/leader in a position of authority, a group of people, or an entire nation's national homeland security interest), or for example, such a similar type of system wide seizure could also, for example, be used as a medium through which individuals could be duped into inappropriate disclosure of highest confidential or classified information to the wrong entities or at a system level, convincing another system that appropriate actions permissions which the seized system has access to is sufficient evidence that requested sensitive information is being released to only appropriate individuals, besides the extremely unfortunate and contemptible efforts of unscrupulous individuals to prey upon the fears, concerns, and sympathies of the unsuspecting public in times of tragedy and/or associated fear. What is potentially equally as worrisome is the possibility of such individuals to do further damage, for example, by: